

Amendments to the Claims

1 Claim 1 (currently amended): In a computing environment having a connection to a network, a
2 computer program product for securely propagating security credentials from a trusted master
3 registry, the computer program product embodied on one or more computer-readable media and
4 comprising:

5 computer-readable program code means for establishing a secure connection between a
6 client and a password synchronization agent (PSA);

7 computer-readable program code means for transmitting an identifier of a user and an
8 identifying secret of the user from the client to the PSA over the secure connection;

9 computer-readable program code means for validating the user with the trusted master
10 registry using the transmitted user identifier and identifying secret, on request of the PSA; and

11 computer-readable program code means for propagating the identifying secret of the user
12 directly from the PSA to one or more target registries if the validation succeeds.

1 Claim 2 (original): The computer program product according to Claim 1, further comprising:

2 computer-readable program code means for establishing a second secure connection
3 between the PSA and the trusted master registry; and

4 computer-readable program code means for using the second secure connection for the
5 validating of the user.

1 Claim 3 (original): The computer program product according to Claim 1, further comprising:

2 computer-readable program code means for establishing additional secure connections

Serial No. 09/613,983

-5-

Docket RSW9-2000-0044-US1

3 between the PSA and each of the target registries; and

4 computer-readable program code means for using the additional secure connections for
5 the propagating of the identifying secret.

1 Claim 4 (original): The computer program product according to Claim 1, wherein the master
2 registry stores password synchronization policy information, and wherein the computer-readable
3 program code means for propagating the identifying secret further comprises computer-readable
4 program code means for identifying the target registries using the stored password
5 synchronization policy information for the user.

as
1 Claim 5 (original): The computer program product according to Claim 1, wherein the master
2 registry stores password synchronization policy information, and wherein the computer-readable
3 program code means for propagating the identifying secret further comprises computer-readable
4 program code means for identifying the target registries using the stored password
5 synchronization policy information for a user group of which the user is a member.

1 Claim 6 (original): The computer program product according to Claim 1, wherein the computer-
2 readable program code means for establishing the secure connection further comprises computer-
3 readable program code means for authenticating the PSA to the client.

1 Claim 7 (original): The computer program product according to Claim 2, wherein the computer-
2 readable program code means for establishing the second secure connection further comprises

Serial No. 09/613,983

-6-

Docket RSW9-2000-0044-US1

3 computer-readable program code means for authenticating the master registry to the PSA.

1 Claim 8 (original): The computer program product according to Claim 3, wherein the computer-
2 readable program code means for establishing additional secure connections further comprises
3 computer-readable program code means for authenticating the one or more target registries to the
4 PSA.

1 Claim 9 (currently amended): The computer program product according to Claim 1, wherein the
2 computer-readable program code means for validating further comprises:

3 computer-readable program code means for performing a security function on the
4 identifying secret of the user, wherein the security function comprises one of (i) a one-way
5 hashing algorithm or (ii) an encryption algorithm;

6 computer-readable program code means for using the user identifier to locate a
7 previously-stored identifying secret of the user which was stored by the master registry; and

8 computer-readable program code means for concluding that the validation succeeds if
9 comparing the located identifying secret is identical to a result of performing the security function.

1 Claim 10 (original): The computer program product according to Claim 1, wherein the computer-
2 readable program code means for validating further comprises computer-readable program code
3 means for invoking an authenticated LDAP bind or other native authentication mechanism of the
4 master registry, wherein the identifier of the user and the identifying secret of the user are passed
5 to the master registry, thereby causing the master registry to validate the passed identifier and

Serial No. 09/613,983

-7-

Docket RSW9-2000-0044-US1

6 identifying secret and return a result which reports a success or failure of the validation.

1 Claim 11 (original): The computer program product according to Claim 1, wherein the PSA has
2 administrative authority for performing operations at the one or more target registries.

1 Claim 12 (currently amended): The computer program product according to Claim 1, further
2 comprising:

3 computer-readable program code means for obtaining a new value from the user to be
4 used as the propagated identifying secret if the validation succeeds; and

5 computer-readable program code means for substituting this new value for the identifying
6 secret prior to operation of the computer-readable program code means for propagating.

1 Claim 13 (currently amended): A system for securely propagating security credentials from a
2 trusted master registry, comprising:

3 means for establishing a secure connection between a client and a password
4 synchronization agent (PSA);

5 means for transmitting an identifier of a user and an identifying secret of the user from the
6 client to the PSA over the secure connection;

7 means for validating the user with the trusted master registry using the transmitted user
8 identifier and identifying secret, on request of the PSA; and

9 means for propagating the identifying secret of the user directly from the PSA to one or
10 more target registries if the validation succeeds.

Serial No. 09/613,983

-8-

Docket RSW9-2000-0044-US1

1 Claim 14 (original): The system according to Claim 13, further comprising:
2 means for establishing a second secure connection between the PSA and the trusted
3 master registry; and
4 means for using the second secure connection for the validating of the user.

1 Claim 15 (original): The system according to Claim 13, further comprising:
2 means for establishing additional secure connections between the PSA and each of the
3 target registries; and
4 means for using the additional secure connections for the propagating of the identifying
5 secret.

1 Claim 16 (original): The system according to Claim 13, wherein the master registry stores
2 password synchronization policy information, and wherein the means for propagating the
3 identifying secret further comprises means for identifying the target registries using the stored
4 password synchronization policy information for the user.

1 Claim 17 (original): The system according to Claim 13, wherein the master registry stores
2 password synchronization policy information, and wherein the means for propagating the
3 identifying secret further comprises means for identifying the target registries using the stored
4 password synchronization policy information for a user group of which the user is a member.

Serial No. 09/613,983

-9-

Docket RSW9-2000-0044-US1

1 Claim 18 (original): The system according to Claim 13, wherein the means for establishing the
2 secure connection further comprises means for authenticating the PSA to the client.

1 Claim 19 (original): The system according to Claim 14, wherein the means for establishing the
2 second secure connection further comprises means for authenticating the master registry to the
3 PSA.

Q5
1 Claim 20 (original): The system according to Claim 15, wherein the means for establishing
2 additional secure connections further comprises means for authenticating the one or more target
3 registries to the PSA.

1 Claim 21 (currently amended): The system according to Claim 13, wherein the means for
2 validating further comprises:
3 means for performing a security function on the identifying secret of the user, wherein the
4 security function comprises one of (i) a one-way hashing algorithm or (ii) an encryption algorithm;
5 means for using the user identifier to locate a previously-stored identifying secret of the
6 user which was stored by the master registry; and
7 means for concluding that the validation succeeds if comparing the located identifying
8 secret is identical to a result of performing the security function.

1 Claim 22 (original): The system according to Claim 13, wherein the means for validating further
2 comprises means for invoking an authenticated LDAP bind or other native authentication

Serial No. 09/613,983

-10-

Docket RSW9-2000-0044-US1

3 mechanism of the master registry, wherein the identifier of the user and the identifying secret of
4 the user are passed to the master registry, thereby causing the master registry to validate the
5 passed identifier and identifying secret and return a result which reports a success or failure of the
6 validation.

1 Claim 23 (original): The system according to Claim 13, wherein the PSA has administrative
2 authority for performing operations at the one or more target registries.

1 Claim 24 (currently amended): The system according to Claim 13, further comprising:
2 means for obtaining a new value from the user to be used as the propagated identifying
3 secret if the validation succeeds; and
4 means for substituting this new value for the identifying secret prior to operation of the
5 means for propagating.

1 Claim 25 (currently amended): A method for securely propagating security credentials from a
2 trusted master registry, comprising steps of:
3 establishing a secure connection between a client and a password synchronization agent
4 (PSA);
5 transmitting an identifier of a user and an identifying secret of the user from the client to
6 the PSA over the secure connection;
7 validating the user with the trusted master registry using the transmitted user identifier and
8 identifying secret, on request of the PSA; and

Serial No. 09/613,983

-11-

Docket RSW9-2000-0044-US1

9 propagating the identifying secret of the user directly from the PSA to one or more target
10 registries if the validation succeeds.

1 Claim 26 (original): The method according to Claim 25, further comprising steps of:
2 establishing a second secure connection between the PSA and the trusted master registry;
3 and
4 using the second secure connection for the validating of the user.

as
1 Claim 27 (original): The method according to Claim 25, further comprising steps of:
2 establishing additional secure connections between the PSA and each of the target
3 registries; and
4 using the additional secure connections for the propagating of the identifying secret.

1 Claim 28 (original): The method according to Claim 25, wherein the master registry stores
2 password synchronization policy information, and wherein the step of propagating the identifying
3 secret further comprises the step of identifying the target registries using the stored password
4 synchronization policy information for the user.

1 Claim 29 (original): The method according to Claim 25, wherein the master registry stores
2 password synchronization policy information, and wherein the step of propagating the identifying
3 secret further comprises the step of identifying the target registries using the stored password
4 synchronization policy information for a user group of which the user is a member.

Serial No. 09/613,983

-12-

Docket RSW9-2000-0044-US1

1 Claim 30 (original): The method according to Claim 25, wherein the step of establishing the
2 secure connection further comprises the step of authenticating the PSA to the client.

1 Claim 31 (original): The method according to Claim 26, wherein the step of establishing the
2 second secure connection further comprises the step of authenticating the master registry to the
3 PSA.

as
1 Claim 32 (original): The method according to Claim 27, wherein the step of establishing
2 additional secure connections further comprises the step of authenticating the one or more target
3 registries to the PSA.

1 Claim 33 (currently amended): The method according to Claim 25, wherein the step of validating
2 further comprises:
3 performing a security function on the identifying secret of the user, wherein the security
4 function comprises one of (i) a one-way hashing algorithm or (ii) an encryption algorithm;
5 using the user identifier to locate a previously-stored identifying secret of the user which
6 was stored by the master registry; and
7 concluding that the validation succeeds if comparing the located identifying secret is
8 identical to a result of performing the security function.

1 Claim 34 (original): The method according to Claim 25, wherein the step of validating further

Serial No. 09/613,983

-13-

Docket RSW9-2000-0044-US1

2 comprises the step of invoking an authenticated LDAP bind or other native authentication
3 mechanism of the master registry, wherein the identifier of the user and the identifying secret of
4 the user are passed to the master registry, thereby causing the master registry to validate the
5 passed identifier and identifying secret and return a result which reports a success or failure of the
6 validation.

as
1 Claim 35 (original): The method according to Claim 25, wherein the PSA has administrative
2 authority for performing operations at the one or more target registries.

1 Claim 36 (currently amended): The method according to Claim 25, further comprising steps of:
2 obtaining a new value from the user to be used as the propagated identifying secret if the
3 validation succeeds; and
4 substituting this new value for the identifying secret prior to operation of the propagating
5 step.
